Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources

Sebastian Philipp Neumann [1,2,*] Thomas Scheidl,[1,2] Mirela Selimovic [1,2] Matej Pivoluska [1,3,4] Bo Liu,[5]
Martin Bohmann [1,2] and Rupert Ursin [1,2,†]

[1]*Institute for Quantum Optics and Quantum Information Vienna, Boltzmanngasse 3, 1090 Vienna, Austria*
[2]*Vienna Center for Quantum Science and Technology, Boltzmanngasse 5, 1090 Vienna, Austria*
[3]*Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic*
[4]*Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*
[5]*College of Advanced Interdisciplinary Studies, NUDT, Changsha 410073, People's Republic of China*

Quantum key distribution (QKD) allows unconditionally secure communication based on the laws of quantum mechanics rather than assumptions about computational hardness. Optimizing the operation parameters of a given QKD implementation is indispensable in order to achieve high secure key rates. So far, there exists no model that accurately describes entanglement-based QKD with continuous-wave pump lasers. We analyze the underlying mechanisms for QKD with temporally uniform pair-creation probabilities and develop a simple but accurate model to calculate optimal tradeoffs for maximal secure key rates. In particular, we find an optimization strategy of the source brightness for given losses and detection-time resolution. All experimental parameters utilized by the model can be inferred directly in standard QKD implementations, and no additional assessment of device performance is required. Comparison with experimental data shows the validity of our model. Our results yield a tool to determine optimal operation parameters for already existing QKD systems, to plan a full QKD implementation from scratch, and to determine fundamental key rate and distance limits of given connections.

I. INTRODUCTION

Quantum key distribution (QKD) is a method of creating a secret and random one-time pad for two remote users usable for unconditionally secure encryption of messages [1,2]. Since its first proposal in 1984 [3], intense research has pushed QKD ever closer to real-life realizations. It has been shown via free-space links on ground [4–6] and from space [7] as well as for long-distance fiber links [8] and in network configurations [9,10]. Many different schemes have been proposed in recent decades, such as entanglement-based protocols (E91 [11] and BBM92 [12]), and twin-field [13] and decoy-state prepare-and-send implementations [14]. Unlike prepare-and-measure protocols, entanglement-based applications have the advantage of being able to create their quantum states in a single coherent process based, for example, on spontaneous parametric down-conversion. Therefore, no quantum random number generators or other electronic inputs are required. Thus, provably no information about the individual photon state exists before the actual measurement. In this sense, entanglement-based protocols exploit the quantum nature of the correlations necessary for QKD on the most fundamental level and can be extended to device-independent QKD [15]. QKD with entangled photons also allows quantum network configurations with many users using one and the same sending apparatus, an entangled-photon source (henceforth simply referred to as "source") [10]. There are two fundamentally different ways to operate such a source: by creating the photon pairs with a continuous-wave (CW) or a pulsed pump laser. Up to now, no in-depth model exists for the prediction of key rates and the calculation of optimal source brightness for CW sources. A model describing sources pumped with a pulsed laser was published in 2007 [16] and has been the state of the art ever since. In such pulsed schemes, all photon pairs are found in discrete and evenly spaced time modes depending on the laser's repetition rate. This rate can be tuned independently of the pulse intensity, allowing one to individually address photon creation rate and multipair emission. Due to the broad frequency spectra in a pulsed-pump scheme, dispersion effects in the optics have to be accounted for, especially in the nonlinear crystals where the entangled photons are created.

This model of pulsed operation can be applied to CW pumped sources with limited accuracy only, as will be shown below. CW pumping has several advantages compared to pulsed-pump schemes, especially in the context of fiber-based QKD: first, the spectrum of the down-converted photons is narrower, thus reducing dispersion effects in both source and transmission channels [17]. Second, additional high-precision

---

*sebastian.neumann@oeaw.ac.at
†rupert.ursin@oeaw.ac.at

time synchronization is not needed as the temporal correlation peak can be precisely determined using a delay histogram. And third, damage to the source optics due to high-intensity pulses can be avoided.

In this paper, we present a model that accurately describes CW-pumped entanglement-based QKD systems. Importantly, all necessary inputs to the model can be read directly from experimentally available data, without the need of any additional assumptions. Our approach allows one to calculate optimal brightness values and coincidence window lengths as well as the resulting final key rate. Hence, the present results are of particular importance for state-of-the-art entanglement-based QKD applications. Comparison with experimental data demonstrates the validity of our model. Although we are focusing here on polarization-encoded BBM92 implementations, our approach can be extended to other degrees of freedom, which is, however, outside of the scope of this paper.

The paper is structured as follows: in Sec. II, we explain the basic working principle of polarization-encoded BBM92. We then develop our model in Sec. III by first introducing parameters for an idealized model (Sec. III A), modifying them to account for experimental imperfections (Sec. III B) and then combining them into the final model to calculate the expected secure key rates (Sec. III C). We optimize the key rate with regard to pair creation rate and temporal detection tolerance and compare our model with experimental data (Sec. IV). Concluding, in Sec. V we discuss our findings and present optimal parameters to maximize key rates.

II. WORKING PRINCIPLE OF ENTANGLEMENT-BASED QKD

Entanglement-based QKD protocols such as BBM92 [12] rely on entanglement between distant physical systems, in our case specifically in the polarization degree of freedom of a photon pair. In an idealized scenario, one can create maximally entangled photon pairs which form a so-called Bell state, e.g.,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A \otimes |H\rangle_B + |V\rangle_A \otimes |V\rangle_B), \qquad (1)$$

where H (V) denotes horizontal (vertical) polarization and the subscripts signify the recipient of the single photon traditionally called Alice (A) and Bob (B). We choose this state because of the fact that it is correlated in the mutually unbiased linear polarization bases HV and DA (diagonal and antidiagonal), where $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. The following model can however be used for any Bell state, if the correlations are adapted accordingly.

Alice and Bob measure their photons randomly and independently from each other either in the HV or the DA basis. The basis choice can in practice be realized actively or passively. Actively means that Alice and Bob switch their measurement bases depending on the outputs of a quantum random number generator. A QKD implementation with passive basis choice uses probabilistic beamsplitters to direct the photons to either a HV or a DA measurement, both of which are realized simultaneously. In the course of the paper, we will assume active basis choice unless noted otherwise. In

any case, Alice and Bob record outcome (H, $D = 0$ and V, $A = 1$) and measurement basis for each event. By communicating about their measurement bases only, Alice and Bob can discard those recorded events where they measured in different bases and therefore see no correlation between their bit outcome ("sifting"). For the other events, they can expect perfect correlation, and thus use their sifted bit strings for key creation. By checking a randomly chosen subset of their sifted measurement outcomes to make sure that correlations have not degraded, Alice and Bob can rule out the existence of an eavesdropper.

In a real experiment, however, perfect Bell states such as in Eq. (1) do not exist. The polarization correlations are degraded through optical imperfections of the source and the detectors, which result in bit and/or phase flips. Also, in practice it is not possible to distinguish each and every consecutively emitted entangled pair from one another due to imperfections in temporal detection, as discussed below. We call such temporally irresolvable emissions "multipairs."[1] Multipairs degrade the quantum correlations necessary to create a secure key, since detection of a multipair photon at Alice does not unambiguously herald the detection of its entangled—and therefore perfectly correlated—partner photon at Bob (and vice versa). Instead, with a certain probability, the photon is wrongly identified as being correlated with a photon from another pair, which leads to errors. Based on these considerations, in what follows, we will define the parameters necessary to calculate the performance of a CW-QKD system. All of these parameters can easily be obtained from experimental detection results, thus making our model ideally suited for direct implementation in real-world applications.

III. MODELING QKD WITH CW-PUMPED SOURCES

For developing the model, we will start out with an idealized polarization-encoded CW-QKD protocol introducing the basic parameters (Sec. III A). In Sec. III B, we will extend this consideration by taking into account noise counts and multipair effects. We then use the experimental quantities defined in this way to calculate error rate and secure key rate (Sec. III C).

A. Idealized CW-QKD system

The most general CW-pumped source setup uses a photon source creating an average number of entangled photon pairs per time unit. This quantity is called brightness B, for which we use the unit counts per second (cps) instead of hertz to emphasize the random nature of the emission process. We assume the probability of photon-pair creation to be uniformly distributed in time, as is justified in the case of CW pumping [18,19].

The entangled photons are spatially separated and sent to communication partners Alice and Bob, where they are detected with overall channel probabilities η_A and η_B, respectively. Although these probabilities are composed of the

---

[1]Unlike in pulsed-source BBM92 [16], coherent emission of n-pair states is negligible in the case of sources using CW pump lasers due to the photons' temporal multimode character [18].

source's intrinsic heralding efficiency [20], the channel and coupling losses, the detection optics' transmission, and the detectors' dead times and efficiencies, we will consider each η_i as one single entity in the following calculations, sometimes referred to as system efficiency. This is because isolating individual loss effects is difficult in a real experiment and not required for our model.

As a result of these definitions, the average local photon detection rate of Alice and Bob, the so-called single counts, can be written, respectively, as

$$S_A^t = B\eta_A \text{ and } S_B^t = B\eta_B, \qquad (2)$$

where we ignore noise counts for now. Note also that dead-time-induced losses, unlike other effects contributing to the η_i, are a function of detector count rates S_i^t and therefore of the brightness B, which has to be taken into account for low-loss scenarios (see Appendix B 1).

Naturally, two photons of a pair must be detected in order to observe their polarization correlation, i.e., use them for generating a cryptographic key. The rate of such two-photon events, which we call "true coincident counts" or "true coincidences,"[2] is given as

$$CC^t = B\eta_A\eta_B, \qquad (3)$$

where we again preliminarily ignore noise counts. Using Eqs. (2) and (3), the η_i can be calculated as [20]

$$\eta_A = \frac{CC^t}{S_B^t} \text{ and } \eta_B = \frac{CC^t}{S_A^t}. \qquad (4)$$

The η_i are sometimes also called "heralding efficiency," since they give the probability that the detection of one photon in one arm announces, or "heralds," the detection of a photon in the other arm. One can also define a total heralding efficiency $\eta = \sqrt{\eta_A\eta_B}$.

Imperfections of source, polarization compensation, and optical detection system lead to erroneous polarization measurement outcomes, i.e., two-photon events which do not comply with the expected Bell state. We call the probability of such an erroneous measurement e^{pol}. It consists of contributions of the individual polarization error probabilities e_A^{pol} and e_B^{pol} of Alice and Bob, respectively:

$$e^{pol} = e_A^{pol}(1 - e_B^{pol}) + e_B^{pol}(1 - e_A^{pol}). \qquad (5)$$

It should be noted that measuring the wrong bit value at Alice *and* Bob still counts as a valid measurement, since it is impossible in principle for the experimenter to distinguish such an event from a correctly measured true coincidence. In most practical implementations, it is more convenient to read

---

[2]Please note that *true coincidences* are not a measurable quantity, since the experimenter cannot distinguish between a true or an accidental coincidence in principle. Even if an accidental coincidence does not conform to the expected correlations, it cannot be unambiguously identified as "accidental," since "true" coincidences can also be measured erroneously [see Eq. (5)]. Therefore, the notion of true pairs is solely a useful concept for our model, describing the photons that actually provide the nonclassical correlations necessary for QKD.

e^{pol} directly from the experimental data instead of quantifying the e_i individually (see Appendix A).

B. Noise-afflicted CW-QKD system

In a real-world entanglement-based QKD implementation, the crucial source of error is not e^{pol}, which can be kept below 1% in modern applications [21], but the unavoidable registration of uncorrelated multipair photons which have lost their partner, and/or noise counts as coincidences. Such erroneous coincidences are called "accidental coincidence counts." To calculate the accidental coincidence rate for BBM92 with a CW pump, first one needs to modify Eq. (2) to account for dark counts DC_i in the detectors:

$$S_A^m = S_A^t + DC_A \text{ and } S_B^m = S_B^t + DC_B \qquad (6)$$

where S_i^m are the actually measured count rates. Note that stray light, residual pump laser light, intrinsic detector dark counts, or any other clicks which do not originate from source photons all have the same effect for our purposes. Therefore, we include all such clicks in the DC_i. In a real experiment, Alice and Bob require at least two detectors each to be capable of distinguishing orthogonal quantum states. In Eq. (6), we assume that Alice and Bob each own identical detectors the photon and dark count rates of which can simply be added; for the case of nonidentical detectors and polarization dependent detection efficiency, see Appendix B 3.

Alice and Bob identify coincidences by looking for simultaneous detection times (accounting for a certain constant delay t_D caused by different photon travel times and electronic delays). There are three main effects that can degrade the fidelity of this identification: the detection system's finite timing precision, the coherence length of the photons, and chromatic dispersion effects in fiber, which delay photons of different wavelengths with respect to each other [17]. These effects cause a spread of the photons' temporal correlation function, the full width at half maximum (FWHM) of which we call t_Δ. Because in any real experiment $t_\Delta > 0$, Alice and Bob need to define a so-called coincidence window t_{CC}. It can be understood as the temporal tolerance allowed for the difference in detection time of two correlated photons.

It follows that there is a possibility of confusing uncorrelated detector clicks with true coincidences. This possibility can be calculated, since it depends on t_{CC} and the S_i^m. Assuming independent Poissonian photon statistics at Alice and Bob, one can define the mean number of clicks at Alice and Bob, respectively, per coincidence window as

$$\mu_A^S = S_A^m t_{CC} \text{ and } \mu_B^S = S_B^m t_{CC}. \qquad (7)$$

Most single-photon detectors used today are not photon-number resolving. Therefore, the chance of an accidental coincidence being registered can be approximated by the probability of *at least* one detection event taking place at each of them:

$$P^{acc} = (1 - e^{-\mu_A^S})(1 - e^{-\mu_B^S}), \qquad (8)$$

where we use the fact that the click probability is given by $(1 - e^{-\mu_i^S})$; see Refs. [22,23]. This expression for P^{acc} provides a good estimate for the accidental coincident-count probabilities in high-loss regimes. For low-loss scenarios it
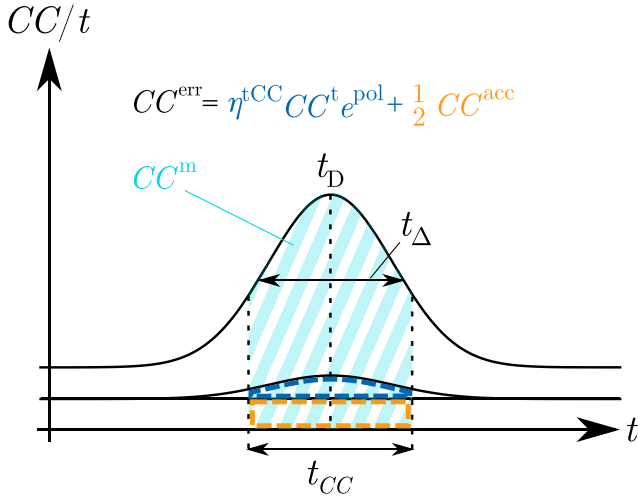
FIG. 1. Number of coincidences per time unit for different relative measurement times. t_{D} is the delay between Alice and Bob and t_Δ is the FWHM of the temporal distribution, both of which are constant. The magnitude of the freely selectable coincidence window t_{CC} not only determines the number of total coincidences $\mathrm{CC^m}$, but also the QBER E, i.e., the ratio of erroneous ($\eta^{t\mathrm{cc}}\mathrm{CC^t}e^{\mathrm{pol}}$) plus half of all accidental ($\frac{1}{2}\mathrm{CC^{acc}}$) coincidence counts to $\mathrm{CC^m}$.

needs to be adapted as it overestimates the probability of accidental coincidence counts by also counting true coincidences as accidental (see Appendix B 2). For $\mu_i^S \ll 1$, Eq. (8) can be simplified to

$$P^{\mathrm{acc}} \approx \mu_{\mathrm{A}}^S \mu_{\mathrm{B}}^S. \qquad (9)$$

The rate of accidental coincidences per second is therefore

$$\mathrm{CC^{acc}} = \frac{P^{\mathrm{acc}}}{t_{\mathrm{CC}}} \approx \frac{\mu_{\mathrm{A}}^S \mu_{\mathrm{B}}^S}{t_{\mathrm{CC}}} = S_{\mathrm{A}}^{\mathrm{m}} S_{\mathrm{B}}^{\mathrm{m}} t_{\mathrm{CC}}. \qquad (10)$$

Note that, since we assume *at least* one detector click per receiver for an accidental count to happen, we take into account the fact that in a real experiment with several detectors there can be more than one click per coincidence window (see Appendix B 2). In that case, a random bit value has to be assigned [24,25], which has the same error probability as an accidental count and can therefore be seen as a part of Eq. (10). Also note that $\mathrm{CC^{acc}}$ depends quadratically on B, but $\mathrm{CC^t}$ linearly. Thus, noise increases faster than the desired signal when increasing B, which gives an intuitive understanding why simply pumping the source with higher power can only enhance the key rate up to a certain degree (see Sec. IV).

It is not only accidental coincidences which depend on the choice of t_{CC}. If it is chosen in the order of the timing imprecision t_Δ, true coincidences will be cut off and lost due to the Gaussian shape of the $g^{(2)}$ intensity correlation with FWHM t_Δ between Alice's and Bob's detectors (see Fig. 1).

This $g^{(2)}$ function can be modeled as a normal distribution

$$j(t, t_\Delta, t_{\mathrm{D}}) = \frac{2}{t_\Delta}\sqrt{\frac{\ln(2)}{\pi}}\exp\left[-\frac{4\ln(2)}{t_\Delta^2}(t - t_{\mathrm{D}})^2\right] \qquad (11)$$

with delay t_{D}. t_Δ is the resulting timing imprecision between Alice's and Bob's measurements, i.e., it is the convolution of

detector jitter, chromatic dispersion, and coherence time of the photons at both Alice and Bob. To arrive at the loss which true coincidences suffer due to the coincidence window, one can carry out the integration

$$\eta^{t\mathrm{cc}} = \int_{-t_{\mathrm{CC}}/2}^{t_{\mathrm{CC}}/2} j(t, t_\Delta, t_{\mathrm{D}} = 0)dt \qquad (12)$$

$$= \mathrm{erf}\left[\sqrt{\ln(2)}\frac{t_{\mathrm{CC}}}{t_\Delta}\right]. \qquad (13)$$

Here, $\eta^{t\mathrm{cc}}$ is the proportion of true coincidences which fall into the chosen coincidence window t_{CC} and are thus identified as coincidences in the experiment. In this sense, $\eta^{t\mathrm{cc}}$ can be interpreted as coincidence-window dependent detection efficiency. Now we can define the actually measured coincidences as

$$\mathrm{CC^m} = \eta^{t\mathrm{cc}}\mathrm{CC^t} + \mathrm{CC^{acc}}. \qquad (14)$$

This is the total number of detector events per second that Alice and Bob use to create their key. But obviously, a subset of these events occurring with rate $\mathrm{CC^{err}}$ actually does not show correlations in accordance with Eq. (1)—first, all those correlated photons which are measured erroneously; and second, on average half of all accidental coincidence counts:

$$\mathrm{CC^{err}} = \eta^{t\mathrm{cc}}\mathrm{CC^t}e^{\mathrm{pol}} + \frac{1}{2}\mathrm{CC^{acc}}. \qquad (15)$$

C. Error rate and secure key rate

From the quantities defined above, one can now calculate the quantum bit error rate (QBER E), i.e., the ratio of erroneous coincidences to total coincidences:

$$E = \frac{\mathrm{CC^{err}}}{\mathrm{CC^m}} = \frac{\eta^{t\mathrm{cc}}\mathrm{CC^t}e^{\mathrm{pol}} + \frac{1}{2}\mathrm{CC^{acc}}}{\eta^{t\mathrm{cc}}\mathrm{CC^t} + \mathrm{CC^{acc}}}. \qquad (16)$$

As a side remark, the commonly used parameter "visibility" V relates to E as $V = 1 - 2E$ [1]. Figure 1 shows a geometrical interpretation of Eq. (16). Coincidences correspond to different areas under the graphs, which are restricted by the chosen coincidence window. On one hand, it is desirable to increase the ratio of the light blue area to the combined dark blue and orange ones, which is equivalent to decreasing E. This can be done by decreasing t_{CC}, since the Gaussian-shaped $\mathrm{CC^m}$ (dark blue curve) scales more favorable in this case than the uniformly distributed accidental coincidence counts $\mathrm{CC^{acc}}$. On the other hand, reducing t_{CC} means that $\eta^{t\mathrm{cc}}$ reduces the total number of coincidences which can be used for key creation.

In order to evaluate the tradeoff between these two effects, we will analyze the secret key rate in the limit of infinitely many rounds—the so-called asymptotic key rate.[3] Alice and Bob choose randomly between measurement settings in the *HV* and *DA* bases. Let us denote the probability that Alice and Bob measure in the same basis as q. Only in this case, the polarization measurement outcomes at Alice and Bob are

---

[3]Where finite-key effects are of interest, one will have to take into account the total number of coincidences per block size and modify Eq. (17) accordingly. This might lead to different optimal experimental parameters satisfying Eq. (20). Nevertheless, the experimental parameter definitions of Sec. III B will be applicable also in this case.
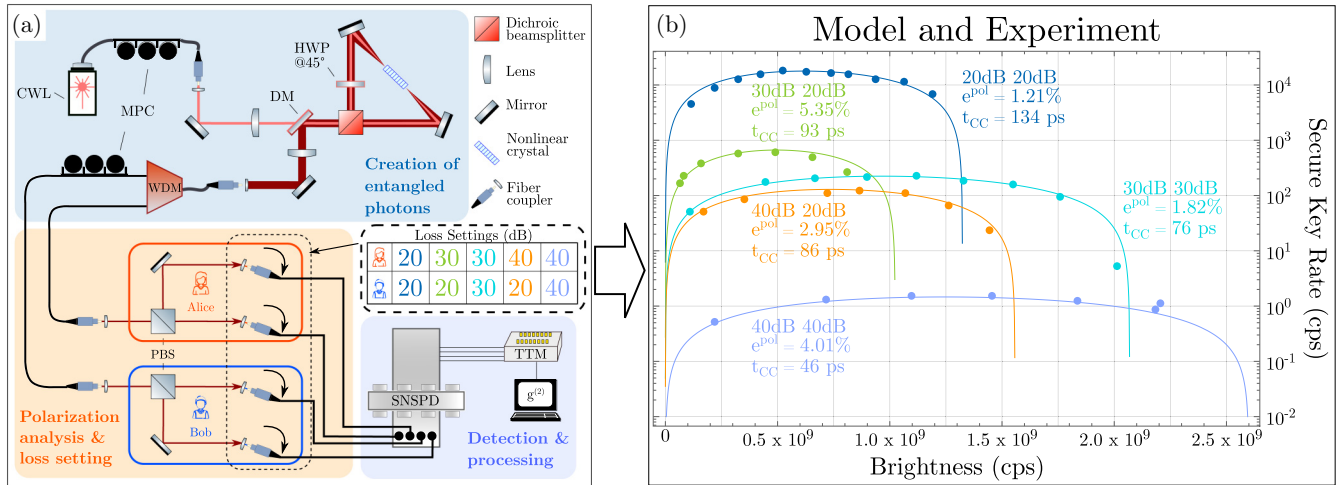
FIG. 2. (a) Setup used to create and detect polarization-entangled photon pairs for quantum key distribution. Top: A periodically poled lithium niobate nonlinear crystal is placed inside a Sagnac-type interferometer loop and pumped bidirectionally with a 775-nm continuous-wave laser (CWL). Via spontaneous parametric down-conversion (SPDC), it produces H-polarized photon pairs. The polarization of the counterclockwise pair is rotated to V via a half-wave plate (HWP) set to 45°. It interferes with the clockwise pair at the beamsplitter and is directed to a single-mode-fiber (SMF) coupler by use of a dichroic mirror (DM). An off-the-shelf wavelength division demultiplexer (WDM) separates the two photons and directs them to two polarization analyzing modules (bottom left). The manual polarization controller (MPC) in the pump fiber is used to set the photon pairs' Bell state of Eq. (1). The MPC in Alice's arm compensates for the random polarization rotation in Bob's arm in order to arrive at the desired correlations. Alice and Bob perform an orthogonal polarization state measurement on their photon using polarizing beamsplitters (PBS) the output modes of which are coupled into SMF and directed to superconducting nanowire single-photon detectors (SNSPD). Different loss scenarios are set by purposeful misalignment of the fiber couplers. Detection events of the SNSPD channels are recorded using a time-tagging module (TTM). From these tags, the $g^{(2)}$ correlation function can be determined from delay histograms between the channels, and secure key rates can be calculated. (b) Comparison of our model (solid lines) and experimentally obtained data points (dots) for different loss settings and polarization measurement errors e^{pol}. SNSPD jitter values vary with count rate, which we account for in the model calculations by making t_Δ a linear function of B. The data show that our model correctly predicts secure key rates over a wide range of losses, polarization errors, and brightness values.

correlated. All other coincidences have to be discarded. Therefore, the rate of coincidence rounds left for postprocessing is equal to $q\mathrm{CC}^m$. Subsequently, Alice and Bob reveal a small fraction of measurement outcomes in both bases to estimate the error. Now we can finally evaluate the amount of achievable key per second as [16]

$$R^{\mathrm{s}} = q\mathrm{CC}^m[1 - f(E_{\mathrm{bit}})\mathrm{H}_2(E_{\mathrm{bit}}) - \mathrm{H}_2(E_{\mathrm{ph}})], \quad (17)$$

where H_2 is the binary entropy function defined as

$$\mathrm{H}_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \quad (18)$$

E_{bit} and E_{ph} are the bit and phase error rates, which are measurement-basis-dependent rates of measurement outcomes incompatible with the maximally entangled state described in Eq. (1). $f(E_{\mathrm{bit}})$ is the bidirectional error correction efficiency which takes into account how much of the key has to be sacrificed due to the fact that postprocessing is performed in finite blocks. In order to asses the validity of our model against an actual experiment, both the sifting rate q and efficiency $f(E_{\mathrm{bit}})$ need to be defined. We assume that the measurement settings of Alice and Bob are chosen uniformly, and thus $q = 1/2$. Further, we choose a realistic value of $f(E_{\mathrm{bit}}) = 1.1$ [26]. Finally, since in our model the noise parameters are independent of measurement settings, we can set $E_{\mathrm{bit}} = E_{\mathrm{ph}} = E$. With these choices, the key rate

formula becomes

$$R^{\mathrm{s}} = \tfrac{1}{2}\mathrm{CC}^m[1 - 2.1\mathrm{H}_2(E)]. \quad (19)$$

From Eq. (19) follows immediately that there is a fundamental limit $E_{\mathrm{max}} \approx 0.102$, above which no key creation is possible. In the following section we maximize R^{s} depending on the parameters discussed up to now. Importantly, all parameters used in this optimization can be directly determined in real-life experiments, which is explained in detail in Appendix A. Finally, note that the key rate formula can be adjusted using Eq. (17) to take into account measurement setting dependent losses as well; see Appendix B 4 for details.

IV. COMPARISON TO EXPERIMENTAL DATA

For realistic applications, the η_i, the optical error e^{pol}, the dark counts DC_i, and the temporal imprecision t_Δ cannot be modified freely. Two important parameters however can be chosen by the experimenter: brightness B and coincidence window t_{CC}. The experimenter can vary B up to a certain level by changing the laser pump power in the source. With laser powers of many hundreds of milliwatts, brightness values of up to 10^{10} cps are feasible with current state-of-the-art sources [21]. The coincidence window t_{CC} can in principle be chosen at will. It follows that for each QKD scenario there is an optimal choice of B and t_{CC} which maximizes R^{s} of Eq. (19). Figure 2 shows a comparison of our model and

experimental values, where t_{CC} has been numerically optimized for each curve with regard to the highest obtainable key rate and is then kept constant for every curve.

The data were collected using a Sagnac-type source of polarization-entangled photons in the telecom C band. For a detailed description of such a source's working principle, we refer the reader to Ref. [21]. After passing wavelength division multiplexing (WDM) filters of 18.4-nm FWHM centered about 1531 and 1571 nm, the photons impinge on single-photon superconducting nanowire detectors (SNSPDs) of the Single Quantum Eos series with detection efficiencies of 80% and dead times as low as 40 ns according to the manufacturer. The detectors were connected to the time tagging module (TTM) Ultra 8 by Swabian Instruments. To keep the analysis of the model simple, we measured only in one superposition basis. Losses were introduced by controlled misalignment of the single-mode-fiber (SMF) couplers. All experimental parameters were determined by using count rates, coincidence rates, and temporal histograms of the single-photon detections only, with no need of additional "external" characterization (see Appendix A). Since the timing jitter of nanowire detectors strongly depends on the count rates they measure, linear fits of the jitter change depending on brightness have been included in the model.

The data show excellent agreement with our model's predictions. The losses introduced in the measurements range from 40 to 80 dB in total, with different distributions along the channels. Note that the two loss scenarios with equal total loss of 60 dB (orange and turquoise curve) perform very differently. Assuming $DC_A = DC_B$,[4] symmetric loss is preferable to asymmetric loss because the probability of a partnerless photon matching with a dark count is reduced in this case. In Fig. 2, this effect on the two 60-dB curves is, however, exaggerated due to different polarization errors e^{pol}, which we set via a manual polarization controller (MPC) to show the model's validity for different parameter regions. The total losses are equivalent to in-fiber distances between 200 and 400 km. Nevertheless, our model can be applied to all kinds of quantum channels, including, e.g., free-space satellite connections, where variation of the channel attenuation [27,28] can be integrated in our model in a straightforward manner.

We want to emphasize that in any case our optimization strategy works exclusively with experimentally measurable quantities that can be inferred directly from the actual QKD implementation (see Appendix A). Furthermore, the presented model can be used during the planning phase of an experiment to devise optimal working parameters based on specification sheets. While several calculations are approximated in our model, it shows excellent agreement with the experimental data. This is proof of its usefulness in a wide range of experimental parameters. For a more extensive treatment of phenomena that might become necessary in certain parameter

───────

[4]If DC_A and DC_B differ strongly, loss asymmetry can actually be beneficial. In a simplified view, this is because higher dark count rates matter less when occurring at detectors with higher single count rates. However, since in most scenarios neither loss nor dark counts can be chosen freely, we omit an in-depth discussion of this effect.
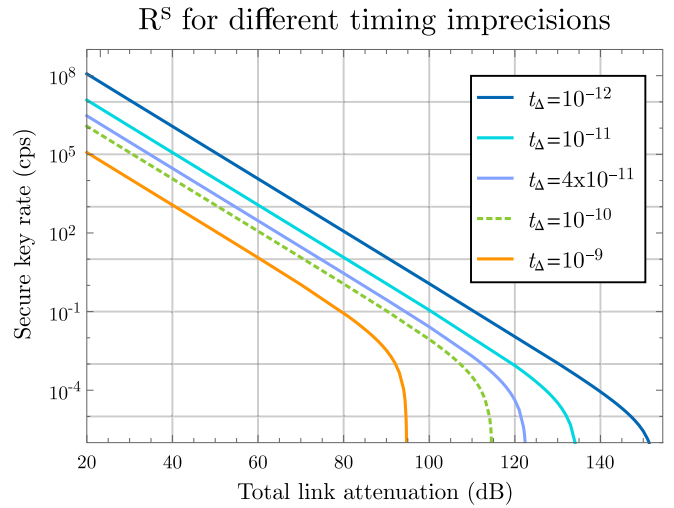

FIG. 3. Key rate R^s vs total symmetric link loss $\eta_A \eta_B$ for different timing imprecision values t_Δ. Brightness B and coincidence window t_{CC} have been optimized for every point of every curve. Dark counts $DC_A = DC_B = 250$ cps are kept constant for each of the four detectors per communication partner. Also polarization error $e^{pol} = 1\%$ is constant for all curves. Lower t_Δ allows both for higher key rates and longer maximum distance, since CC^{acc}, the main source of errors, is directly proportional to t_Δ. Note that the dotted green curve ($t_\Delta = 10^{-10}$ ps) is the same curve as the equally colored one in Fig. 4.

regimes, such as dead-time effects, low-loss channels, and nonidentical detectors, we refer the reader to Appendix B.

V. OPTIMIZATION OF QKD WITH A CW-PUMPED SOURCE

Now that we have shown the validity of our model in different parameter scenarios, we want to use it to illustrate the limits and potential of CW-QKD. Therefore, we numerically maximize both B and t_{CC} for every point on the curves in Figs. 3 and 4, i.e.,

$$\frac{\partial}{\partial B} \frac{\partial}{\partial t_{CC}} R^s(B, t_{CC}; \eta_i, e^{pol}, DC_i, t_\Delta) = 0 \qquad (20)$$

is fulfilled continuously. Figure 3 shows the maximum obtainable key rate assuming symmetric loss for different jitter values. Lower jitter allows for a smaller coincidence window, which in turn allows for higher brightness values and thus key rates. Note that no matter the jitter value there is an abrupt drop to zero key after a certain amount of loss. This is because dark counts will inevitably induce a minimum accidental coincidence count value $CC^{acc}_{min} = DC_A DC_B t_{CC}$. In a regime of high loss, this constant value can mask true coincidences if $\eta^{t_{CC}} CC^t \lesssim 10 CC^{acc}_{min}$. In this case, key creation is frustrated. Figure 4 now shows how CC^{acc}_{min} is reduced with lower dark count values. For the hypothetical case of $DC_i = 0$, the accidental coincidences CC^{acc} can be decreased to arbitrarily low values by reducing the brightness B. Although this also decreases maximum key rates beyond the point of usefulness, they never drop to zero, as indicated by the dark blue curve. When comparing Figs. 3 and 4, it becomes apparent that in a real-world scenario reducing the timing imprecision t_Δ is
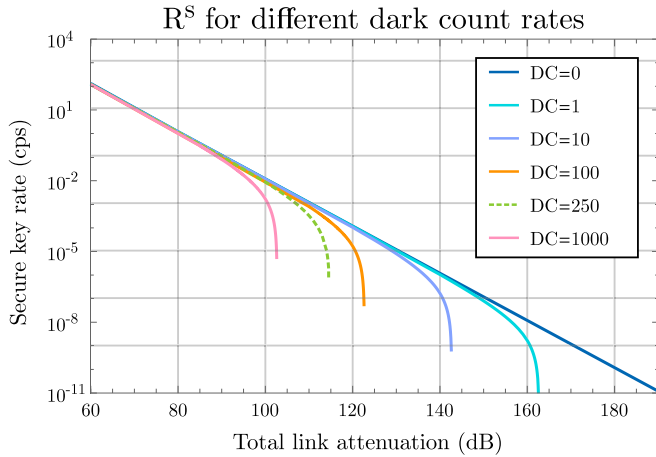
R$^{\mathrm{s}}$ for different dark count rates

FIG. 4. Key rate R^{s} vs total symmetric link loss $\eta_A \eta_B$ for different dark count rates DC per detector and four detectors per communication partner. The timing imprecision t_Δ is kept constant at 100 ps and the polarization error at $e^{\mathrm{pol}} = 1\%$. As can clearly be seen, reducing detector noise counts effectively only increases the maximum achievable distance. In the case of no dark counts (dark blue curve), there exists no distance limit, since t_{CC} can in principle be set arbitrarily small, thus keeping the error rate below $E_{\max}$ for any loss. Note that the dotted green curve (DC = 250) is the same curve as the equally colored one in Fig. 3.

more important than reducing the dark counts. This is because lower DC_i can only increase the maximum distance in high-loss regimes, where key rates are extremely low already. To increase the key rate for a given loss, it is more favorable to lower t_Δ in most cases.

We would also like to emphasize that when wrongly using the model for pulsed-source BBM92 by Ma *et al.* [16] to estimate key rates for a CW-pumped implementation one arrives at erroneous results, even when trying to adapt it. One could try to do so by replacing the mean photon number per pulse 2λ with the average photon number per coincidence window
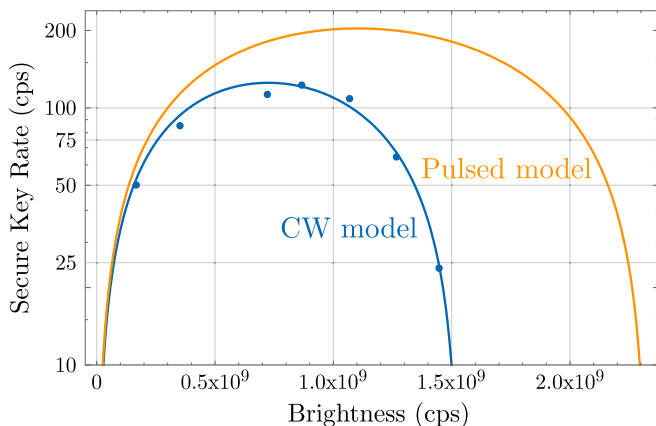

FIG. 5. Comparison of 40- and 20-dB experimental data with the secure key predicted by our model (blue line) vs an adapted version of the pulsed-source model from Ref. [16] (orange line). Since temporal detection imprecision does not enter the pulsed-source model, it overestimates both the maximum key rate and the optimal brightness value.

$\mu = Bt_{CC}$ and changing the multipair probability of Eq. (5) in Ref. [16] to a Poissonian distribution. Since doing so ignores any effects of temporal uncertainty, the results differ strongly, as can be seen in Fig. 5.

VI. CONCLUSION

In this paper, we have presented a comprehensive and accurate model of continuous-wave entanglement-based quantum key distribution. Our model allows one to estimate and optimize the performance of any given CW-QKD system by extracting experimental parameters from the recorded detections only, without the need to perform any additional characterization of the experiment. It also allows one to compare different devices and find the optimal solution for a given quantum link. For a given QKD setup, the model can accurately estimate the optimal settings of brightness and coincidence window to extract the maximal possible key and thus enhance the performance of the implementation. Furthermore, the presented approach is readily extendable to BBM92 based on entanglement in other degrees of freedom. We are confident that our easy-to-implement model will be used as an important design and optimization tool for CW-QKD links.

APPENDIX A: PARAMETER ESTIMATION

There are numerous ways to estimate the parameters discussed in this paper. When planning a QKD link from scratch, one has to rely on data sheets and fiber loss measurements. However, one can also estimate all parameters with the same QKD equipment used for the experiment, if already available.

Directly accessible parameters for the experimenter are t_{CC} (since it is a free variable to be chosen by the experimenter), S_i^{m}, and CC^{m}. The delay t_D between Alice's and Bob's detection times can be found out by calculating a delay histogram of single counts at Alice and Bob and determining the location of the histogram peak (see Fig. 6). From the same histogram, the (total) timing imprecision t_Δ can be read from the peak's FWHM (less CC^{acc}). It should be mentioned that SNSPD jitter depends on both the detector's bias current and its count rate, and exhibits the lowest specified values for high current and low count rates only. This dependency has been included in the model of Fig. 2 by using a linear fit of t_Δ vs B rather than a constant jitter value.

The dark counts DC_i can be determined by blocking the source of photons and observing the S_i^{m}, which are equal to the DC_i for $B = 0$ [see Eqs. (2) and (6)]. Note however that stray light from the pump beam cannot be observed with this method. To do so, one either needs filters that block just
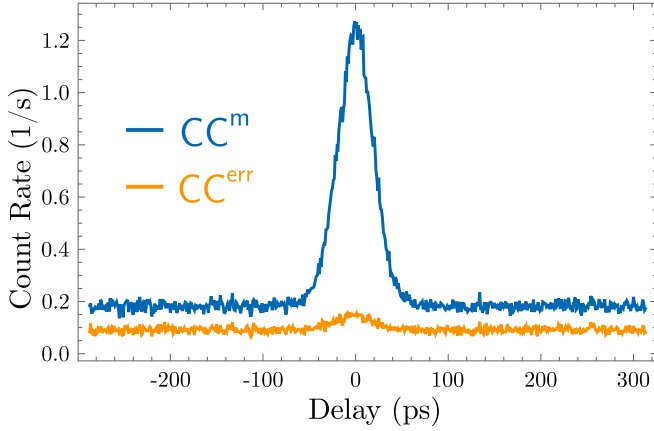
FIG. 6. Measured $g^{(2)}$ correlation histogram for the 40- and 40-dB loss setting. CC^m contains all measured counts for all possible channel combinations, where all histograms have been shifted by their respective delays t_D. CC^{err} only shows undesired correlations, i.e., between polarization measurements not in accordance with Eq. (1). The orange curve's small peak around zero corresponds to erroneous polarization measurements, while the noise floor is equivalent to accidental coincidence counts CC^{acc} (see Fig. 1).

the SPDC wavelength, or the possibility to frustrate SPDC without blocking or misdirecting the laser, e.g., by changing the crystal temperature. Especially for long-distance single-mode-fiber links designed for the SPDC wavelength, it is safe to assume that pump light is sufficiently suppressed at the detectors.

For the following calculations, it is necessary to determine CC^t (for a certain brightness). Especially in the case of low loss and low jitter, this can be done experimentally by lowering the brightness to a value where $CC^{acc} \to 0$ and therefore $CC^m \to CC^t$. Alternatively, CC^{acc} can be subtracted from CC^m: either by calculation using Eq. (10) or experimentally by changing t_D to a value far from the actual coincidence peak, while keeping t_{CC} constant. In absence of CC^t, the measured CC^m become equal to CC^{acc}. For all these approaches, it is important to choose t_{CC} large enough such that $\eta^{t_{CC}} \to 1$; as a rule of thumb, $t_{CC} = 3t_\Delta$ is sufficient.

Now to determine the optical error e^{pol}, one can use the methods just described to eliminate CC^{acc} in Eq. (16) such that $E \approx e^{pol}$.

The heralding efficiencies or transmission factors η_i can be calculated using Eq. (4), where again CC^t and S_i^t have to be determined in advance by subtracting CC^{acc} and DC_i.

Finally, also the brightness B can be calculated using CC^t and S_i^t via

$$B = \frac{S_A^t S_B^t}{CC^t}. \tag{A1}$$

Note that for this calculation of the η_i and B, dead-time effects have not been taken into account. Thus, even if the CC^{acc} are simply measured and subtracted, one should take care to operate the source at sufficiently low pump power (see Appendix B 1).

If it should be necessary to incorporate dead-time effects, the most efficient way to determine $t_\dagger$ is to calculate an auto-correlation histogram in time of each detector channel while

subjecting it to photons with Poissonian emission statistics. The temporal stretch for which no correlations are found is the detector channel's dead time.

APPENDIX B: ADDITIONAL CORRECTIONS

1. Dead-time loss

In scenarios with high detector count rates, an additional loss factor might be considered to account for the detectors' dead time $t_\dagger$ [29]:

$$\eta_i^{t_\dagger} = \frac{1}{1 + B\eta_i t_\dagger/d}. \tag{B1}$$

Here d is the number of (identical, see Appendix B 3) detectors deployed per communication partner. This effective loss cannot simply be considered as a constant contribution to η_i, since it is a function of S_i^m and therefore B. For $B\eta_i t_\dagger/d < 0.02$, $\eta_i^T \approx 1$ holds. Note that the estimation of B can be compromised if this assumption is not justified due to low loss, high brightness, and/or long detector dead time.

Another result of dead-time loss is that the definition of the μ_i^S in Eq. (7) needs to be modified, since photons arriving at the detectors during the dead time do not contribute to S_i^m. One therefore needs to modify the CC^{acc} in Eq. (10) to

$$CC^{acc}_{t_\dagger} \approx \frac{S_A^m S_B^m t_{CC}}{\eta_A^{t_\dagger} \eta_B^{t_\dagger}} \tag{B2}$$

where we assume $DC_i \ll S_i^t \eta_i$, which is reasonable in the high single-count regimes where dead-time effects become important.

2. Accidental coincidence probability

Equation (8) slightly overestimates the probability of accidental coincidence counts. Since it assumes completely independent photon statistics at Alice and Bob, *any* photon contributes to CC^{acc}, regardless of whether it has lost its partner or not. Thus, here we want to give a more extensive description P_{ext}^{acc}, which is well approximated by P^{acc} in Eq. (9) for $\eta_i \ll 1$. We start by defining the probability of a coincidence happening per coincidence window, P^{CC^t}:

$$\begin{aligned} P^{CC^t} = \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} \sum_{i=1}^{n} & \left[\left[(1 - \eta_A)^{i-1}(1 - \eta_B)^{i-1} \eta_A \eta_B \right] \right. \\ & \times \left(1 - \frac{\eta_A}{2} \right)^{n-i} \left(1 - \frac{\eta_B}{2} \right)^{n-i} \\ & \left. \times \left(1 - \frac{P_A^{DC}}{2} \right) \left(1 - \frac{P_B^{DC}}{2} \right) \right] \end{aligned} \tag{B3}$$

where $\mu = Bt_{CC}$ is the average number of photon pairs created per coincidence window before any loss, and $P_i^{DC} = DC_i t_{CC}$ are the probabilities of a noise count happening at Alice and Bob, respectively, per coincidence window. This formula takes into account the Poissonian emission and dark count statistics. Multipair emissions can still yield a valid measurement if photons get lost in a way that two correlated photons end up at the detectors before all others (first factor inside the square brackets). However, if photons emitted after the

true pair, but inside the coincidence window, are detected as well, they can in some cases eliminate a true coincidence (second line). The divisions by 2 come from the fact that if the later photon detection occurs in the same detector as the true photon detections this case cannot be distinguished from a true coincidence. If it clicks in the other detector, a random bit value has to be assigned, i.e., only this case has to be counted as an accidental. Dark counts can also occur in the presence

of a true pair, eliminating a valid coincidence in the same way as photons arriving later, which gives rise to the factors in the third line. As a side remark, in the case of passive basis choice using beamsplitters, there are four instead of two detectors deployed; accordingly, the factor $1/2$ has to be replaced by $3/4$.

Using $P^{\mathrm{CC}'}$, the actual probability of detecting an accidental coincidence per coincidence window reads

$$P_{\mathrm{cor}}^{\mathrm{acc}} = 1 - e^{-\mu}\big[1 - P_{\mathrm{A}}^{\mathrm{DC}}P_{\mathrm{B}}^{\mathrm{DC}}\big] - P^{\mathrm{CC}'} - \sum_{n=1}^{\infty} e^{-\mu}\frac{\mu^n}{n!}\Big[(1-\eta_{\mathrm{A}})^n + (1-\eta_{\mathrm{B}})^n - (1-\eta_{\mathrm{A}})^n(1-\eta_{\mathrm{B}})^n$$

$$- (1-\eta_{\mathrm{A}})^n[1-(1-\eta_{\mathrm{B}})^n]P_{\mathrm{A}}^{\mathrm{DC}} - [1-(1-\eta_{\mathrm{A}})^n](1-\eta_{\mathrm{B}})^n P_{\mathrm{B}}^{\mathrm{DC}} - (1-\eta_{\mathrm{A}})^n(1-\eta_{\mathrm{B}})^n P_{\mathrm{A}}^{\mathrm{DC}}P_{\mathrm{B}}^{\mathrm{DC}}\Big]. \tag{B4}$$

The formula can be understood as follows: The accidental coincidence probability $P_{\mathrm{cor}}^{\mathrm{acc}}$ can be seen as all those two-click events that did not originate from a true pair. We proceed by subtracting from probability 1 all events which are no accidental coincidences.

Thus, in the first line, we subtract the probability of no photon pair being emitted, corrected by the case of two dark counts producing a coincidence. We also subtract all correct coincidences according to Eq. (B3). Then we subtract the sum over all remaining pair emission probabilities which are not the vacuum state, not a true coincidence, and not an accidental count. In the second line, we count those cases where no accidental coincidence happens since in at least one arm no click occurs. Since the possibility of both detectors not clicking is included in both $(1 - \eta_A)^n$ and $(1 - \eta_B)^n$, it has to be subtracted. This subtraction avoids mistakenly counting the case of all photons lost twice.

In lines 3 and 4 of Eq. (B4), we have to re-add the cases where dark counts cause an accidental coincidence by "replacing" a photon. All other dark count cases are already included in the first line of the equation—either as part of $P^{\mathrm{CC}'}$ or in 1, since a dark count happening when an accidental coincidence would have occurred anyway does not change their statistics.

For $\eta_i \ll 1$, one can approximate $P_{\mathrm{cor}}^{\mathrm{acc}}$ with P^{acc} from Eq. (9), which actually constitutes an upper bound for Eq. (8).

3. Nonidentical detectors

In our model, we assume Alice and Bob, respectively, to use identical detectors for their orthogonal polarization measurements. It has recently been shown [30] that vast differences in detector performance do not necessarily degrade the security of a QKD protocol. However, different detection efficiencies lead to asymmetric single-count rates and therefore different accidental coincidence rates for different polarization correlations. On top of this, different detector jitters lead to different $\eta^{t_{\mathrm{CC}}}$ for each correlation. These asymmetries and differences of used detectors can lead to a deviation from the reported model.

To account for such imbalances one has to define two heralding efficiencies per communication partner, which we denote by $\eta_{\mathrm{A}j}$ and $\eta_{\mathrm{B}k}$, where j and k indicate the detectors. Following Eq. (3), one can now differentiate true coincidence

values:

$$\mathrm{CC}_{jk}^{\mathrm{t}} = B\eta_{\mathrm{A}j}\eta_{\mathrm{B}k}, \tag{B5}$$

for which

$$\sum_{j,k=1}^{2} \mathrm{CC}_{jk}^{\mathrm{t}} = \mathrm{CC}^{\mathrm{t}} \tag{B6}$$

holds. Additionally, one has to subdivide the S_i^{m} while accounting for different dark count rates

$$S_{\mathrm{A}j}^{\mathrm{m}} = B\eta_{\mathrm{A}j} + \mathrm{DC}_{\mathrm{A}j}, \tag{B7}$$

$$S_{\mathrm{B}k}^{\mathrm{m}} = B\eta_{\mathrm{B}k} + \mathrm{DC}_{\mathrm{B}k} \tag{B8}$$

where similarly

$$S_{\mathrm{A}}^{\mathrm{m}} = \sum_{j=1}^{2} S_{\mathrm{A}j}^{\mathrm{m}} \quad \text{and} \quad S_{\mathrm{B}}^{\mathrm{m}} = \sum_{k=1}^{2} S_{\mathrm{B}k}^{\mathrm{m}} \tag{B9}$$

and assign different accidental coincidence rates to different detector combinations:

$$\mathrm{CC}^{\mathrm{acc}} = \sum_{j,k=1}^{2} \mathrm{CC}_{jk}^{\mathrm{acc}} = \sum_{j,k=1}^{2} S_{\mathrm{A}j}^{\mathrm{m}} S_{\mathrm{B}k}^{\mathrm{m}} t_{\mathrm{CC}}. \tag{B10}$$

To take into account different detector jitters, one arrives at different values of $t_{\Delta jk}$, which require an adaptation of the coincidence window loss of Eq. (13):

$$\eta_{jk}^{t_{\mathrm{CC}}} = \mathrm{erf}\left[\sqrt{\ln(2)}\frac{t_{\mathrm{CC}}}{t_{\Delta jk}}\right]. \tag{B11}$$

In this case, Eq. (14) becomes

$$\mathrm{CC}^{\mathrm{m}} = \sum_{j,k=1}^{2} \big[\eta_{jk}^{t_{\mathrm{CC}}}\mathrm{CC}_{jk}^{\mathrm{t}} + \mathrm{CC}_{jk}^{\mathrm{acc}}\big], \tag{B12}$$

and similarly Eq. (15) can be written as

$$\mathrm{CC}^{\mathrm{err}} = \sum_{j\neq k}^{2} \big[\eta_{jk}^{t_{\mathrm{CC}}}\mathrm{CC}_{jk}^{\mathrm{t}}e^{\mathrm{pol}} + \mathrm{CC}_{jk}^{\mathrm{acc}}\big]. \tag{B13}$$

Here we assume a correlated Bell state ($\phi^{+/-}$) in the respective basis. For anticorrelated ones ($\psi^{+/-}$), the indices to be summed over have to be replaced by $j = k$.

4. Key-rate-formula adjustments

Following from the above considerations, in a realistic experiment, one might additionally expect that one of the polarization measurement settings used in the BBM92 protocol is more prone to errors than the other one. Let us assume that this is due to different optical errors e^{pol} which can depend on the measurement basis. As an example, the HV basis often shows higher fidelity than the superposition bases as a result of the source design, which relies on polarizing beamsplitters defining H and V with high extinction (1 : 1000 or better). Because of this, we obtain two values of QBER [see Eq. (16)], one for each measurement setting. Let us denote these with E_{HV} and E_{DA}. If coincidences obtained in the HV basis are used to derive the key, then in Eq. (17) we can set $E_{bit} = E_{HV}$ and $E_{ph} = E_{DA}$. Similarly, for a key derived from coincidences in the DA basis we set $E_{bit} = E_{DA}$ and $E_{ph} = E_{HV}$. If both Alice and Bob choose the HV setting with probability p and the *DA* setting with probability $(1 - p)$, they would obtain two key rates, each in one basis:

$$R_{HV}^s = p^2 CC^m[1 - H_2(E_{DA}) - f(E_{HV})H_2(E_{HV})], \quad (B14)$$

$$R_{DA}^s = (1 - p)^2 CC^m[1 - H_2(E_{HV}) - f(E_{DA})H_2(E_{DA})]. \quad (B15)$$

The total key rate is then the sum of these two key rates, and the total compatible basis choice probability from Eq. (17) is $q = p^2 + (1 - p)^2$.

Another common technique is to use predominantly one of the basis settings and use the other only with very low probability to obtain the estimate on E_{ph}. This is often referred to as the "efficient BB84 protocol" [31]. In the asymptotic setting, one can therefore assume that the probability p to choose the HV basis approaches unity, and the final key rate is

$$R_{efficient}^s = CC^m[1 - H_2(E_{DA}) - f(E_{HV})H_2(E_{HV})]. \quad (B16)$$

Additionally, in some works the authors assume that in the asymptotic setting the block length is also approaching infinity and therefore $f(E_{bit})$ approaches unity [32,33]. Last but not least, even in the case of different error rates, one can in practice use the average error $E = (E_{HV} + E_{DA})/2$ with Eq. (19) to obtain a lower bound on the secret key rate [10,34], since

$$2H_2\left(\frac{E_1 + E_2}{2}\right) \geqslant H_2(E_1) + H_2(E_2) \quad \forall E_i \in [0, 0.5]. \quad (B17)$$

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).

[3] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014).

[4] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, P. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nature Phys. **3**, 481 (2007).

[5] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Nature (London) **488**, 185 (2012).

[6] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, npj Quantum Inf. **7**, 5 (2021).

[7] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, Nature (London) **582**, 501 (2020).

[8] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, Proc. Natl. Acad. Sci. USA **116**, 6684 (2019).

[9] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, Nature (London) **564**, 225 (2018).

[10] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, Ž. Samec, L. Kling, A. Qiu, M. Stipčević, J. G. Rarity, and R. Ursin, Sci. Adv. **6**, eaba0959 (2020).

[11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[12] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[13] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Nat. Photon. **15**, 570 (2021).

[14] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[15] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[16] X. Ma, C. H. F. Fung, and H. K. Lo, Phys. Rev. A **76**, 012307 (2007).

[17] S. P. Neumann, D. Ribezzo, M. Bohmann, and R. Ursin, Quantum Sci. Technol. **6**, 025017 (2021).

[18] H. Takesue and K. Shimizu, Opt. Commun. **283**, 276 (2010).

[19] R. Hošák, I. Straka, A. Predojević, R. Filip, and M. Ježek, Phys. Rev. A **103**, 042411 (2021).

[20] D. N. Klyshko, Sov. J. Quantum Electron. **10**, 1112 (1980).

[21] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, Rev. Sci. Instrum. **92**, 041101 (2021).

[22] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, Phys. Rev. A **95**, 033806 (2017).

[23] M. Bohmann, L. Qi, W. Vogel, and M. Chekhova, Phys. Rev. Research **1**, 033178 (2019).

[24] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

[25] T. Moroder, O. Gühne, N. Beaudry, M. Piani, and N. Lütkenhaus, Phys. Rev. A **81**, 052342 (2010).

[26] D. Elkouss, J. Martínez-Mateo, and V. Martin, Quantum Inf. Comput. **11**, 226 (2011).

[27] D. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **117**, 090501 (2016).

[28] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, Phys. Rev. A **95**, 063801 (2017).

[29] V. Bécares and J. Blázquez, Sci. Technol. Nucl. Install. **2012**, 240693 (2012).

[30] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, Phys. Rev. Research **3**, 013076 (2021).

[31] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

[32] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[33] M. Koashi, New J. Phys. **11**, 045018 (2009).

[34] C. H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).